UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

In the Matter of the Search of

Case Number: 17-M-705

Property described as: premises located at W9564 Cloverleaf Road, Hortonville, State and Eastern District of Wisconsin.

.

APPLICATION & AFFIDAVIT FOR SEARCH WARRANT

I, Brian Judd, a federally deputized U.S. Marshal/ federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Property described as premises located at W9564 Cloverleaf Road, Hortonville, WI, is more particularly described as a single story residence with red and cream colored siding and attached garage. There is a gravel driveway leading to the residence from Cloverleaf Road. (See Attachment A).

located in the Eastern District of Wisconsin there is now concealed: see Attachment B, which constitutes evidence of receipt, distribution, and possession of child pornography in violation of 18 U.S.C. ' § 2252, and 2252A.

The basis for the search warrant under Fed. R. Crim. P. 41(c) is which is:

T evidence of a crime;
T contraband, fruits of a crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The application is based on these facts:

T Continued on the attached pages, which are incorporated by reference.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. ' 3103a, the basis of which is set forth on the attached pages.

Applicants signature
Name and Title: BRIAN JUDD, TFO

Sworn to before me, and signed in my presence.

Date October 16, 2017

City and state: Green Bay, Wisconsin

Judges signature
HONORABLE JAMES R. SICKEL
United States Magistrate Judge
Name & Title of Judicial Officer

AFFIDAVIT

I, Brian Judd, having been duly sworn, depose and state as follows:

1. I have been a Sworn Law Enforcement officer for 17 years with the Sheboygan County Sheriff's Office, and currently hold the rank of Detective. In that position my primary duty is to conduct Forensic Examination of Computers and Digital media. I have also been trained in conducting Peer to Peer child exploitation investigations. I am currently assigned to the Milwaukee Division Child Exploitation Task Force (CETF) with the Federal Bureau of Investigation (FBI). I am charged with conducting investigations of violations of federal law including the receipt, possession, distribution, and production of child pornography. I have gained experience in the conduct of such investigations through prior investigations, formal training, and in consultation with other members of the CETF regarding these matters.

2. As part of my duties with CETFE, I have received TFO/Special Deputy United States Marshal designation, authorizing me to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. Thus, I am considered a federal law enforcement officer able to present and execute federal search warrants.

2. I am participating in an investigation of receipt and possession of child pornography, which is a violation of Title 18, United States Code, Section 2252(a)(2). This affidavit is based upon my personal knowledge, as well as information reported

to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon information gathered from official records, law enforcement reports, and my training and experience.

3. Based upon the information below, I submit probable cause

exists to believe a person accessing the Internet at W9564 Cloverleaf Road, Hortonville, Wisconsin ("SUBJECT PREMISES"), more particularly described in Attachment A, has received and is in possession of child pornography, in violation of Title 18, United States Code, Section 2252(a)(2), and that evidence of this crime, more particularly described in Attachment B, will be found at that location. In addition to the residence, this affidavit seeks authority to search the garage associated with W9564 Cloverleaf Road. This affidavit is intended to only show there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DEFINITIONS

4. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. "Cellular telephone" or "cell phone" means a hand held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and

playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but are not, in and of themselves, legally obscene or do not necessarily depict minors in sexually explicit conduct.

c. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e. "Computer Server" or "Server," is a computer attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

f. "Computer hardware" means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software" is digital information which can be interpreted by a

computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information

(e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the Internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

k. "Hash Value" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a "digital fingerprint" for data. If the data is changed, even slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means the digital photo is an exact copy of the known file.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Internet Service Providers" (ISPs) are commercial organizations in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based

dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

n. "An Internet Protocol address" (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to the electronic storage device may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

o. "Media Access Control" (MAC) address means a hardware identification number which uniquely identifies each device on a network. The

equipment connecting a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter. This MAC address is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

p. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

q. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

r. "Sexually explicit conduct" means actual or simulated (a) sexual

intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

s. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use URLs on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

t. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

5. I consulted with law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, I consulted with FBI SA Matthew Petersen, who has received specialized training as a forensic computer, cellular telephone, and other electronic storage device examiner. SA Petersen has been a forensic computer examiner with the FBI since 1999. SA Petersen has participated in the execution of numerous search warrants and search and seizure operations. SA Petersen has informed me to properly retrieve and analyze electronically stored (computer) data, and to insure accuracy and completeness of such

data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To affect such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, or within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a meaningful form only upon forensic analysis.

6. Based on my knowledge, training, and experience, and after having consulted with SA Petersen, I know computer and other electronic device hardware, peripheral devices, software, electronic files, and passwords may be important to a criminal investigation in three distinct and important respects:

a. The objects themselves may be instrumentalities used to commit the crime;

b. the objects may have been used to collect and store information about crimes (in the form of electronic data); or

c. the objects may be contraband or fruits of the crime.

7. I submit if a computer or other electronic storage device is found on the

premises, there is probable cause to believe information will be saved to that electronic storage device, for the following reasons:

a. Based on my knowledge, training, and experience, I know electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, the data remains on the storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack spaceCthat is, in space on the storage medium that is not currently being used by an active fileCfor long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media in particular, computers internal hard drives contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system

configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

8. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence establishing how electronic storage devices were used, the purpose of their use, who used them, and when.

9. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail

programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device

was remotely accessed, thus inculpating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may show a particular location and have geolocation information incorporated into its file data. Such file data typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculpate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device

user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience it is possible malicious software can be installed on a computer, often without the computer user's knowledge, which can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

10. Based upon my knowledge, training and experience, and after having consulted with SA Matthew Petersen, I know a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

11. In light of these concerns, I hereby request permission to seize the electronic storage devices, associated storage media, and associated peripherals believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

12. I know when an individual uses a computer to commit crimes involving child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of

the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe an electronic storage device used to commit a crime of this type may contain: evidence of how the electronic storage device was used; data sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

DETAILS OF THE INVESTIGATION

13. On August 8, 2017, I, FBI Task Force Officer (TFO) Brian Judd, was informed that TFO Christina Porter was assigned a lead received from FBI Headquarters. TFO Porter and I reviewed the information provided in the lead which included a Cybertip from the National Center for Missing and Exploited Children (NCMEC), a FBI Tactical Targeting Package, and a CD which contained child pornographic images. NCMEC operates the Cyber Tipline and Child Victim Identification Program and they make this information available to law enforcement. NCMEC also works with Electronic Service Providers (ESP), law enforcement and the public to reduce online sexual abuse images.

14. TFO Porter began the investigation by reviewing the Cybertip which stated the submitter of the complaint is Dropbox, Inc. from 185 Berry Street, Suite 400 in San Francisco, CA. The incident type is listed as child pornography and the incident date and time are 01/12/17 at 06:45:36UTC. The account that Dropbox, Inc. was reporting had the following subscriber information:

Email address: ajdolata@gmail.com
Screen/User name: Banana Cow
ESP User ID: 550358587
IP Address: 206.8.80.66 (Login); 11/05/16 at 11:13:00UTC
IP Address: 206.8.80.65 (Login); 11/05/16 at 11:13:31UTC

IP Address: 206.176.207.197 (Login); 11/13/16 at 01:15:17UTC
IP Address: 206.8.80.66 (Login); 12/03/16 at 11:07:10UTC

15. The Cybertip stated that the above listed Dropbox account had uploaded 134 images of suspected child pornography. The Cybertip listed some of the suspected files which were reviewed by Dropbox, Inc. and were publicly available. They provided the following filenames:

c30fe08c-d7cb-4a00-8e92-f9f88bd0b8b0.mp4
e9837acd-9b66-4068-a110-449a4ae7578b.mp4
Untitled 3.02.bmp
CatGoddess (249).jpg
Untitled 3.6.bmp
Untitled 3.7.bmp
CatGoddess (215).jpg

16. NCMEC conducted a geo-lookup for the IP addresses utilized by this account. The IP address of 206.176.207.197 came back to Schofield, WI with an Internet Service Provider (ISP) of Solarus. The IP address of 206.8.80.66 came back to Weyauwega, WI with an ISP of Onvoy. The IP address of 206.8.80.65 came back to Hortonville, WI with an ISP of Onvoy.

17. Per the Cybertip, the NCMEC date from when this complaint was processed was on 02/28/17 at 15:42:44UTC. NCMEC noted that the uploaded files were reviewed and the images appear to be apparent child pornography. An exact law enforcement jurisdiction was undetermined by NCMEC, so the Cybertip was forwarded to the FBI for further investigation.

18. Per the lead, on 04/11/17, MAPA Colleen O'Connor from FBI Headquarters in Alexandria, Virginia, issued an administrative subpoena and non-disclosure order to Dropbox, Inc. in regards to obtaining information pertaining to the email address of ajdolata@gmail.com; Screen/User Name: Banana Cow; ESP User ID

550358587. On 05/01/17 Dropbox provided the following requested information regarding the account:

Name: Banana Cow
Email: ajdolata@gmail.coom
User ID: 550358587
Joined: Tue, 20 Mar 2016 17:53:24 GMT
Subscription Status: Free
Authentication History:

Timestamp (GMT)	IP
Sat, 05 Nov 2016 23:13:00 GMT	206.8.80.66
Sat, 05 Nov 2016 23:13:31 GMT	206.8.80.65
Sun, 13 Nov 2016 01:15:17 GMT	206.176.207.197
Sat, 03 Dec 2016 11:07:10 GMT	206.8.80.66

Mobile Device Information:

Timestamp (GMT)	Model	Carrier
Sat, 05 Nov 2016 23:13:36 GMT	LG-K373	cricket
Tue, 10 Jan 2017 00:55:34 GMT	LG-K373	cricket

19. On 03/02/17, MAPA Colleen O'Connor served an administrative subpoena and non-disclosure order to Google in order to obtain information pertaining to the email account ajdolata@gmail.com. On 03/24/17, Google provided the following requested information regarding the account:

Name: AJ Dolata
e-Mail: AJDolata@gmail.com
Services: Android, Chrome Web Store, Gmail, Google Calendar, Google Chrome Sync, Google Developers Console, Google Docs, Google Drive, Google Hangouts, Google Maps, Google Maps Engine, Google My Maps, Google Payments, Google Photos, Google Play Music, Google Sites, Google Voice, Google+, Has Google Profile, Has Plusone, Location History, Lock SafeSearch, Onetoday, Tasks In Tingle, Web & App Activity, YouTube, iGoogle
Recovery e-Mail: forgeg@gmail.com
Created on: 2012/04/11-23:47:39-UTC
Terms of Service IP: 198.150.183.44, on 2012/04/11-23:47:39-UTC
SMS: +19208105522
Google Account ID: 458621787398
Sample of the IP History: 24.197.229.34 on 2017/01/01-02:02:03-UTC (MaxMind=Charter Communications)
65.25.223.30 on 2017/01/09-19:02:38-UTC (MaxMind=Time Warner Cable)

20. On 03/27/17, MAPA Colleen O'Connor served an administrative subpoena to Charter Communications to obtain information regarding the IP address 24.197.229.34 on 2017/01/01 at 02:02:03-UTC. On 05/05/17 Charter Communications responded with the following requested information:

Target Details: 24.197.229.34, 1/1/2017 2:02:00 AM, GMT
Subscriber Name: Country Inn and Suites
Subscriber Address: 301 Division St. N, Stevens Point, WI 54481-1154
Service Type: RR HSD Activate Date: 6/4/2002 Deactivate Date: 3/9/2017
User Name or Features: jbiad@charter.net, becky@charterinternet.com
Phone number: (715) 345-7000, (715)343-6140, (715) 343-8609, (715)345-7008, (715) 343-6146, (715) 343-6145, (715) 343-6144, (715) 343-6143, (715) 343-6142, (715) 343-6141
Other Details
Other Information: IP address is static.

On 03/28/17 MAPA Colleen O'Connor served an administrative subpoena to Time Warner Cable to obtain information regarding the IP address 65.25.223.30 on 2017/01/09-19:02:38-UTC. On 04/03/17, Time Warner Cable provided the following requested information:

Target Details: 65.25.223.30, 1/9/2017 7:02:00 PM, GMT

Subscriber Name: Midwest Labor
Subscriber Address: 3019 W. Spencer St., Ste 102, Apt. 102, Appleton, WI 54914-5946
Service Type: RR HSD Activate Date: 8/29/2014 Deactivate Date: Still active
User Name or Features: rmanske@edgewood.edu
Phone Number: (920) 364-9454, (920) 609-2526

On 03/27/17, MAPA Colleen O'Connor served an administrative subpoena to AT&T regarding SMS 920-810-5522 (this number was obtained from the Google subpoena results for email ajdolata@gmail.com). On 03/27/17, AT&T provided the following information regarding the request:

Financially Liable Party

Name: Teresa Dolata
Credit Address: W9564 Cloverleaf Rd, Hortonville, WI 54944
Activation Date: 05/21/2016
Billing Party
Account number: 737570307
Name: Teresa Dolata
Billing Address: W9564 Cloverleaf Rd, Hortonville, WI 54944
Account Status: Open Billing Cycle: 21
User Information:
MSISDN: (920) 810-5522
IMSI: 310150819539948
MSISDN Active: 08/28/2016-Current
MSISDN Status: Active

21. TFO Porter advised she then reviewed the Tactical Targeting Package which was included with the lead. The report states that through the analysis of records, obtained through appropriate legal process, the FBI assesses that Anthony James Dolata IV, residing at W9564 Cloverleaf Rd, Hortonville, WI (Outagamie County) is very likely to be involved in the transmission and/or possession of child pornography. The report states that per NCMEC, there are 90 images and 43 videos depicting child pornography which were uploaded to the Dropbox account created by email address ajdolata@gmail.com with screen/user name Banana Cow.

22. Per TFO Porter, the report provides additional information regarding Anthony James Dolata IV. MAPA Colleen O'Connor conducted a Facebook inquiry for Anthony Dolata in Wisconsin and found the possible account URL of https://www.facebook.com/profile.php?id=100007087412822. The profile name is AJ Dolata and the Facebook page shows that he resides in Hortonville, Wisconsin and that he is from Hortonville, Wisconsin. MAPA O'Connor noted that this Facebook account has not been updated since 07/17/14. TFO Porter accessed this Facebook

page on 08/08/17 and the account still had not been updated. There was limited information provided on the profile and no photos of people.

23. MAPA O'Connor conducted an Accurint search on the address of W9564 Cloverleaf Rd., Hortonville, WI and located the resident Anthony James Dolata IV, 11/01/96, SSN of 397-15-4675 and the dates at this address are from October of 2013 through May of 2017. MAPA O'Connor conducted a NCIC check on Anthony and it was determined that he has no criminal history.

24. MAPA O'Connor also requested the images and videos in the Cybertip be reviewed by NCMEC through the Child Victim Identification Program (CVIP) to determine if there are any known victims. A NCMEC analyst reviewed the files and provided these results in Child Identification Report #107357. This report indicates that 79 victims were identified in images and 10 victims were identified in videos.

25. On August 9, 2017 TFO Porter advised she reviewed the images and videos which were provided with the lead from the Dropbox account in question. There were 43 video files and 90 still image files, for a total of 133 files. TFO Porter provided the following as a sample of some of the child pornographic images and videos that she reviewed:

File 0d7da528-e1b8-4dbc-8807-650800af72f1 This is a 14 second video of a nude, white female with dark hair. The female is standing and rubs her breast area with her hand and then rubs her vaginal area with her hand while the camera focuses on her vagina. The female has a small amount of breast development and appears to be between the ages of 10 and 13.

File 3f12a8e4-a047-4082-aca1-b41488cbd860 This is a two minute and two second video of a young, prepubescent white female who is wearing what appears to be pink underwear. The video is a close up of the child's vagina while her legs are spread apart. An adult's hand is rubbing the girl's vaginal area while pulling her underwear aside. Later in the video the adult hand pulls open the girl's vaginal area to expose her even more before the hand continues to rub the area. Based on the size of

the girl in comparison to the size of the adult hand, the girl appears to be between the ages of one and two years old.

File 8b77170a-aa09-4827-9658-ab8549320d83 This is a one minute and 23 second video of a nude, prepubescent white female who is laying on her back and an adult white male is inserting his nude, erect penis into her vagina. The male removes his penis and rubs it. Based on the size of female in comparison to the male, the female appears to be approximately three to five years old.

File CatGoddess (50).jpg This is a still image of a nude, white, prepubescent female who is laying on her back with her legs apart and up in the air, exposing her vaginal area. The female has long, brown hair and is smiling. She lacks muscle development and breast development. She lacks pubic hair. The female appears to be between the approximate ages of nine and eleven years old. There are several images of this female in various poses.

File CatGoddess (79).jpg This is a still image of the same female from file CatGoddess (50).jpg. The female is laying on her back and is nude. Her legs are spread apart, exposing her vaginal area. She is holding a hair dryer in her right hand. Again, the female appears to be between the ages of nine and eleven years old.

File Untitled2.bmp This is a still image of a nude, white, prepubescent female with dark blonde hair. The female is laying on top of an adult, nude male who has an erect penis. The female is holding the base of the male's penis with her right hand and her mouth is around the tip of the penis. The female lacks muscle development and appears to be between the ages of seven and ten years old.

26. Based on her training and experience, TFO Porter believes all of the images and videos provided with the Cybertip are of child pornography.

27. "Dropbox" refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an "offsite" storage medium for data viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted

only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

28. Special Agent Gerald Mullen and TFO Porter applied for a search warrant to Dropbox to obtain all the content of the account, in addition to a search warrant to Google for all of the content within the email account of ajdolata@gmail.com, which was used to create the Dropbox account in question. On September 18, 2017, the search warrants were served to Dropbox and Google.

29. On September 28, 2017, TFO Porter received the Google search warrant results. Per the results, between the dates of March 27, 2017 and September 11, 2017 the following IP addresses were utilized to access the account on a regular bases:

206.8.80.69
206.8.80.66
206.8.80.65
206.8.80.67

TFO Porter used the website whois.arin.net and determined that Onvoy was the company assigned to these IP addresses. TFO Porter conducted a search on the Internet for Onvoy and determined that it is a business that offers VoIP services to small businesses, and enterprise solutions such as call centers and services for carriers. The IP address of 206.8.80.65 was also used to log into the Dropbox account in question on November 5, 2015. The IP address of 206.8.80.66 was used to log into the Dropbox account on November 5, 2016 and on December 3, 2016.

30. Within the Google search warrant results, TFO Porter located various images which indicate that the email account of ajdolata@gmail.com was operated by Anthony J. Dolata IV. For example, TFO Porter located an image of a screen shot

from a Cricket phone which listed Anthony Dolata as the owner of the phone. There were also images of homework with the name of A.J. Dolata on it. Some of the homework was dated from February of 2015, indicating that Anthony was in high school at that time. Anthony's high school senior pictures were located, along with a resume which had Anthony's name and address on it.

31. TFO Porter also located numerous images of anime pornography which were cartoon-like images of creatures with animal heads and human bodies. TFO Porter observed a few videos within the account which appear to be of Anthony masturbating. The majority of the actual emails received in the account were of spam or advertisements.

32. On October 2, 2017, TFO Porter received the Dropbox search warrant results. Included with these results was an excel spreadsheet which included the dates and times account activity took place. The majority of the dates when the account was accessed was in November and December of 2016 and January of 2017. This date range is consistent with the information provided in the Cybertip.

33. TFO Porter observed four folders created within the Dropbox account. The folders were labeled, "Det," "littles taking d," "stuff" and "young vids 12." All of these folders contained only adult or child pornography. There were approximately 17 videos of child pornography located in the "Det" folder. An example is:

File 0798ddll-81c9-4024-9054-b3f5236a3d5f: This is a one minute 30 second video of a girl performing oral (mouth to penis) sex on an adult male. The girl is wearing a plaid shirt and the male is holding her hair back. The girl gagged on the man's penis and the man ejaculated inside of the girl's mouth. The girl then spit out the semen from her mouth. The girl continued to perform oral sex on the man and he again ejaculated inside her mouth. The girl in the video appears to be between the approximate ages of five to eight years of age.

34. In the "littles taking d" folder, TFO Porter observed 23 videos and six of the videos were of child pornography.

35. In the "stuff" folder, TFO Porter observed 142 images/videos. Approximately 124 images/videos were of child pornography. There were 98 images from the same series whereby all the images were titled CatGoddess followed by a different number in parenthesis. The same female is in all of the images in various poses. For example:

File CatGoddess (56): This is a still image of a nude white female who is sitting down with her legs apart and her knees are bent, exposing her vaginal area. The girl is prepubescent and lacks muscle development. She appears to be between the approximate ages of 8 and 12 years old.

36. In the "young vids 12" folder, TFO Porter observed 24 images/videos, all of which were child pornography. For example:

File 3f12a8e4-a047-4082-aca1-b41488cbd860: This is a two minute and two second video of an adult digitally rubbing and penetrating a baby's vagina. The video is a close up of the girl's vagina and then the adult opens the vagina to expose it further. Based on the size of the girl next to the adult hand, she appears to be an infant.

In total, there were about 171 images/videos of child pornography in the Dropbox account, which included the images and videos provided in the Cybertip.

37. TFO Porter and I are aware that Dropbox can be accessed from any electronic device that can access the Internet. If a specific Dropbox account is accessed on a device, remnants of that activity can be located on the device. I am aware that there is information on the electronic device, such as a computer or cellular phone that could show a link between the device and the accessed Dropbox account. More specifically, file paths may be located, indicating that the device connected to the Dropbox account, could

be located on the device utilized. Additionally, the device would have the Dropbox application downloaded onto it, and there would potentially be an icon on the device for Dropbox. If video files are located within a Dropbox account, the video player(s) needed to open such files would also be located on the electronic device in order to play the video file. Examples of video players are VLC or Windows Media Player. The Internet history would contain information regarding when a specific file was searched for and downloaded. I am also aware that when a forensic examination of a cell phone is performed, the software used to provide the examination could provide the file path of specific files' current or previous location which may include Drop Box.

38.

On September 18, 2017, ground surveillance was conducted on the residence at W9564 Cloverleaf Rd. and Anthony Dolata was observed leaving the residence with his father. The surveillance team followed Anthony and his father to Children's Hospital where it appeared that Anthony had a therapy appointment. TFO Porter was advised by FBI Analyst Hannah Loken that she conducted an open source Internet check on the members of the Dolata family and located a Go Fund Me page for Anthony. The Go Fund Me page indicated that Anthony had fallen on March 23, 2017 and suffered from a brain injury, which was likely why Anthony was getting therapy at the hospital.

39. On September 14, 2017, aerial surveillance was conducted at the residence and photos of the residence were taken since the residence has a lengthy driveway and cannot be seen well from the public street.

BACKGROUND ON ELECTRONIC STORAGE DEVICES AND CHILD PORNOGRAPHY

40. Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

41. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many

electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built into the device which allows users to create and store still and video images on the device. Moreover, if the device has Internet connectivity, users can distribute still and video images from the device.

42. Internet-enabled electronic storage devices can connect to other Internet-enabled devices. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via e-mail or through file transfer protocols (FTPs) to anyone with access to an Internet-enabled electronic storage device. Because of the proliferation of commercial services that provide e-mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

43. Electronic storage devices are the ideal repository for child pornography. The amount of information an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on a computer or other electronic storage device. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy

it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

44. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

45. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.

46. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints"

in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

47. Based on my knowledge, training, and experience, I know electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, I believe the images/videos described in paragraphs 39, 40, 41, and 42 above are still located in and can be retrieved from the electronic storage devices at the SUBJECT PREMISES.

CONCLUSION

48. Based on the above, I submit that this affidavit supports probable cause for a warrant to search the premises described in Attachment A and seize the items described in Attachment B.

Dated this 16 day of October 2017.

BRIAN J. JUDD, Task Force Officer
Federal Bureau of Investigation

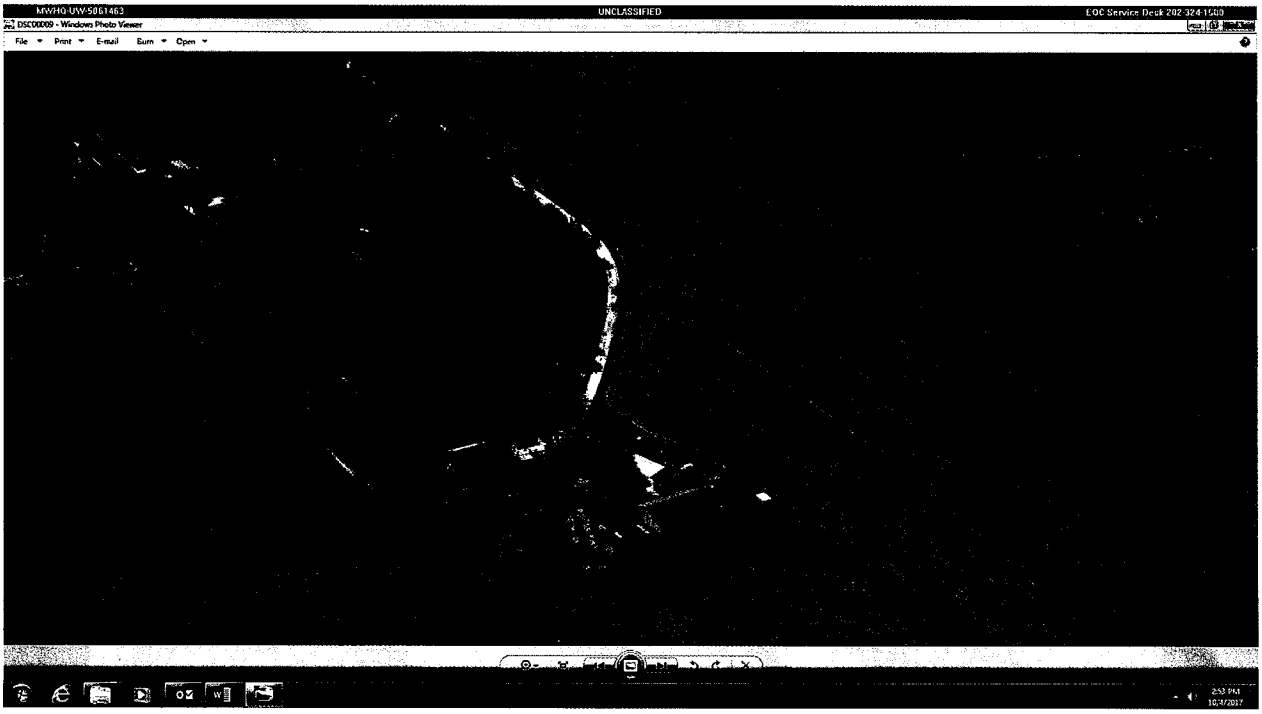
Sworn to before me this 16 day of October 2017.

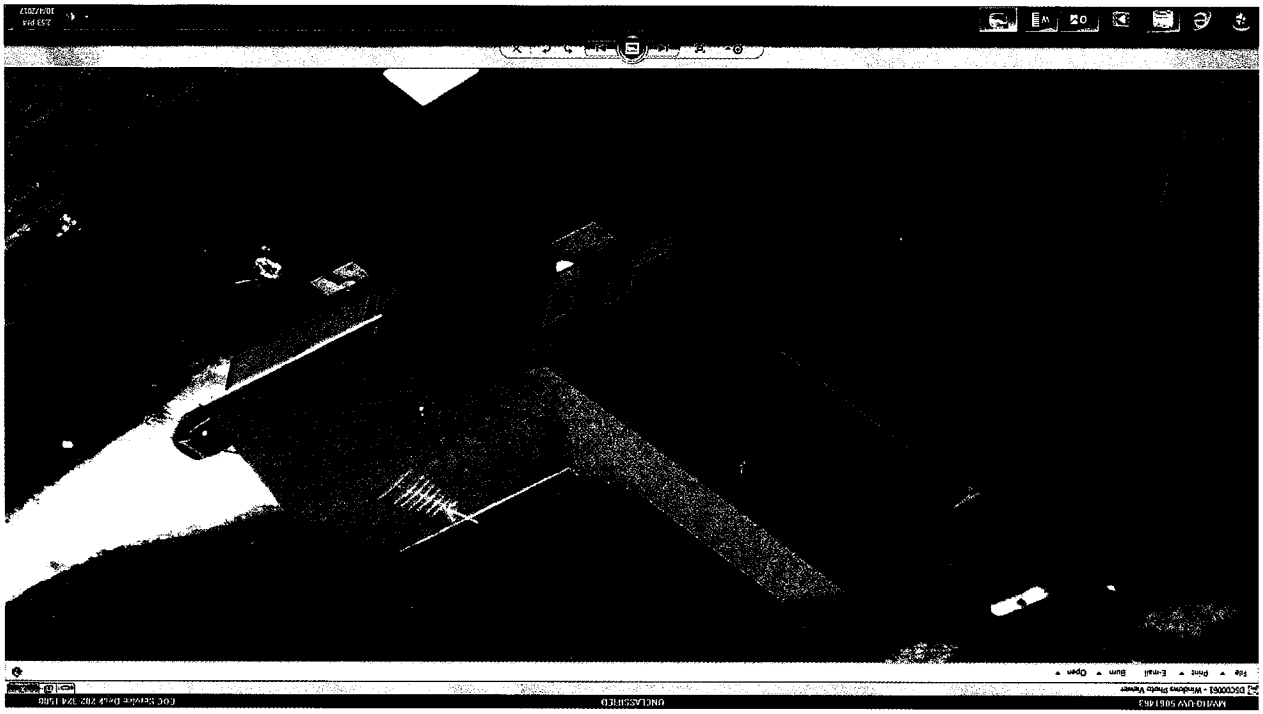
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF THE PROPERTY TO BE SEARCHED

The Subject Premises is located at W9564 Cloverleaf Road, Hortonville, WI. This is a single story residence with attached garage. The asphalt shingles on the roof appear to be light brown in color and the building is in the shape of the letter "L." The central portion of the residence appears to have red colored siding with the attached portions having cream colored siding. The trim around the doors and windows is white in color. The driveway leading to the residence is gravel and the front of the residence is obscured by large trees. Upon approaching the residence from the driveway, the first portion of the structure is the garage, which has two overhead doors, one being a single door and one being a double door. On the rear of the residence there is a bay window adjacent to the back door and green colored deck.





ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography, display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. 2256(2).
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C 2256(2), or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C.

2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256(2).
7. Any and all notes, documents, records or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256(2).
8. Any and all notes, documents, records, or correspondence, in an format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all cameras, film, videotapes or other photographic equipment.
13. Any and all visual depictions of minors.
14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of name so r lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256(2).
15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. Evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. Evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. Evidence of the lack of such malicious software;

    d. Evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

    e. Evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

    f. Evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

    g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

    h. Evidence of the times the electronic storage device was used;

i. Passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. Documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. Contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing communication with the internet, including:

a. Routers, modems, and network equipment used to connect electronic storage devices to the Internet;

b. Records of Internet Protocol addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of Apple brand device(s), such as an iPhone or iPad, found at the premises for purpose of attempting to unlock the devices via Touch ID in order to search the contents as authorized by this warrant.